## REMARKS

Claims 1, 3-10, 13-19, and 21-25 are currently pending in the application. By this response, claims 1, 3, 9, 13-15, 21, and 22 are amended. Additionally, claims 2, 11, 12, and 20 are canceled and claims 23-25 are added for the Examiner's consideration. The amendments and new claims do not add new matter to the application and are fully supported by the specification. For example, support for the amendments and new claims is provided at figures 1A and 1B as well as pages 6, 7, and 9 of the specification. Reconsideration of the rejected claims in view of the following amendments and remarks is respectfully requested.

### *Examiner Interview*

Applicants appreciate the courtesies extended by the Examiner during the telephonic interview with Applicants' undersigned representative conducted on April 10, 2008. During the interview, the rejection of independent claims 1, 9, 15, and 22 under 35 U.S.C. §103(a) was discussed. Possible amendments to the independent claims were also discussed with the Examiner.

### *Amendments to the Claims*

Applicants have amended claims 1, 3, 9, 13-15, 21, and 22 and canceled claims 2, 11, 12, and 20. Applicants are not conceding in this application that those claims are not patentable over the art cited by the Examiner, as the present claim amendments and cancellations are only for facilitating expeditious prosecution of the allowable subject matter noted by the examiner. Applicants respectfully reserve the right to pursue these and other claims in one or more continuations and/or divisional patent applications.

***35 U.S.C. §103 Rejection***

Claims 1-22 were rejected under 35 U.S.C. §103(a) for being unpatentable over U. S. Publication No. 2002/0007460 issued to Azuma ("Azuma") in view of U. S. Patent No. 7,290,288 issued to Gregg, *et al.* ("Gregg"). This rejection is respectfully traversed.

In order to reject a claim under 35 U.S.C. §103(a), the examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness. To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP §2142. Applicants submit that no proper combination of the applied art teaches or suggests each and every feature of the claimed invention.

Claims 1, 9, 15, and 22

Applicants submit Azuma does not include the features of claims 1, 9, 15, and 22 as originally claimed. However, to advance prosecution, Applicants have amended claims 1, 9, 15, and 22 to include the following features.

Claim 1 recites, in pertinent part:

> ... creating a credential string on a portal server, the credential string being an encrypted hash of a session ID;

sending a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;

receiving a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including the credential string; and

sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID.

Claim 9 recites, in pertinent part:

... receiving a UserID and a credential string at an authentication proxy server, the credential string being an encrypted hash of a session ID, which is created at a portal;

sending a confirmation request from the authentication proxy to the portal while maintaining a user password on the portal and avoiding exposing the user password to network resources beyond the portal, the confirmation request includes the credential string;

receiving a response at the authentication proxy for the confirmation request while maintaining the user password on the portal such that the user password is not required to authenticate the User ID, the confirmation request including the credential string; and

validating the UserID using a light weight directory access protocol (LDAP) lookup request and the response.

Claim 15 recites, in pertinent part:

... an authentication proxy which receives requests to authenticate a UserID and a credential string, the credential string being an encrypted hash of a session ID and created on a portal; and

a credential string validation component which receives requests to validate the credential string while maintaining a user password on the portal such that the user password is not required to validate the credential string,

wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal.

Claim 22 recites, in pertinent part:

> ... create a credential string on a portal server, the credential string being an encrypted hash of a session ID;
> send a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;
> receive a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including the credential string; and
> send a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID.

Azuma and Gregg Lack a Credential String

Applicants submit the amendments to claims 1, 9, 15, and 22 are not obvious in view of Azuma and Gregg. In particular, Applicants assert Azuma does not include a credential string being an encrypted hash of a session ID. Instead Applicants submit that Azuma merely stores authentication information, which may include a URL, user ID, password, etc., when it is sent from either a user or a web server.

Azuma performs user authentication operations for websites that require user authentication. This allows users to avoid having to continually sign-on to a system to be authenticated. (Paragraph [0013].) More specifically, Azuma determines whether a user is an authorized user and, if so, allows the user to save data in a proxy user authentication data storage unit. (FIG. 3, A1-A6.) The data saved on the proxy user authentication data storage unit may include a user ID and password. (FIG. 5.) The authenticated user can then send a request for a URL to a user authentication proxy. The user authentication proxy stores the requested URL and the user ID in temporary storage while it connects to a web server. Once connected, the URL is sent to the web server and the web server returns data on the URL to the user authentication proxy. This data is stored in temporary storage and then sent to the user. The user receives this data and sends data required for user authentication. The sent data is received by a user authentication proxy and stored in temporary storage before being sent to the

web server. Once sent to the web server, the data is authenticated. If the web server determines the data is authentic, then a notification is sent to the user via the user authentication proxy and the user authentication proxy saves the information that was previously stored in temporary storage. (Paragraphs [0064] – [0078]; FIG. 6.)

In other words, Azuma uses a user authentication proxy to relay information back and forth between a user and a web server. While relaying the information, a copy of the information is stored in temporary storage until the user is authenticated, i.e., until it is certain the information in temporary storage includes accurate user authentication information. If the information is correct then the information in the temporary storage is saved into the website user authentication data storage unit. Once saved, the user authentication proxy can automatically send the user authentication information associated with the URL to the web server without requiring a user to ever see the authentication request, or submit authentication information. Thus, Azuma allows authentication information, e.g., URL's, user IDs, and passwords, to be automatically handled by a proxy such that users do not have to log in when they enter a secure site.

Applicants submit that Azuma does not include a credential string being an encrypted hash of a session ID. Instead, as described above, Azuma merely stores authentication information, which may include a URL, user ID, password, etc., when it is sent from either a user or a web server. Since the authentication information already includes a URL, Azuma clearly would not create authentication information from an encrypted hash of a URL. Therefore, Applicants submit Azuma does not include a credential string which is an encrypted hash of a session ID.

Additionally, Applicants respectfully submit that Gregg does not make up for the deficiencies of Azuma. Gregg allows an account holder to use a login interface wherein the account holder enters a username, password, and/or a personal identification number. Upon entering this information, the login interface requests that a hardware key interface check for a hardware key, such as a magnetic card, smart card, etc., in order to authenticate the account holder. If the hardware key interface reads the digital

identification from access media, then the hardware key is sent to the log-in interface and the account holder is authenticated. (Col. 16, lines 60-66; FIG 16.) Therefore, Gregg reads a digital identification from an access media as part of the authentication process. However, Gregg does not create a credential string which is an encrypted hash of a session ID. Accordingly, Applicants submit claims 1, 9, 15, and 22 are not obvious in view of Azuma and Gregg.

Azuma and Gregg Fail to Maintain a User Password on a Portal and Fail to Avoid Exposing the User Password to Network Resources Beyond the Portal

Applicants agree with the Examiner's assertion on page 5 of the Office Action that Azuma does not maintain a password at a portal and does not keep the password from being sent to authenticate the UserID. However, Applicants assert that Gregg does not make up for the deficiencies of Azuma. More specifically, Gregg allows an account holder to request transaction services. Once this request is received, a secure transaction server sends the account holder a log-in command, which the account holder uses to enter log-in parameters such as a password, username, and digital ID. These login parameters are sent to a secure transaction server, which forwards them to the transaction clearinghouse as part of an authentication request. If the authentication data is valid then an authentication response is sent from the transaction clearinghouse to the secure transaction server and then to the account holder. This allows the account holder to have access to transaction services. (Fig. 2; Col. 6, lines 15-23.) Therefore, Gregg sends all of the login parameters, including a password, to a secure transaction server and then to a transaction clearinghouse. However, Gregg does not maintain a password at a portal and does not keep the password from being sent to authenticate the UserID.

Azuma and Gregg Fail to Include a Credential String Validation Component that Checks Whether the Credential String has been Previously Received for Validation within a Predetermined Time Period

In addition to the reasons explained above, Applicants further submit claim 15 is not obvious because none of the applied references teach the feature wherein a credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period. In particular, Applicants agree with the Examiner's assertion on page 4 of the Office Action that Azuma fails to teach the feature wherein a credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period. However, Applicants respectfully submit that Gregg does not include this feature.

More specifically, the Examiner is of the opinion that Gregg includes the feature wherein a credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period. To support this assertion, the Examiner has referenced steps 218-220 of FIG. 18 in Gregg. FIG. 18 describes, in part, how Gregg uses a hardware key to provide two or three factor authentication. The hardware key may include a hardware token, magnetic card reader, smart card reader, or biometric identification reader connected to each account holder's client computer or alternatively a secure central processing unit as part of the account holder's client computer capable of reading access media that generates a unique digital ID. (Col. 5, lines 37-45.) Gregg uses this hardware key as a mechanism for authenticating users. Gregg also periodically re-authenticates users involved in active sessions to prevent unauthorized access by someone who no longer has a hardware key. (Col. 17, lines 56-60).

During the re-authentication process, a session validator determines which sessions are active. Once an active session is found, the session validator determines the time the account holder's machine was last polled, or checked, to see if a hardware key is present. If a certain time limit has elapsed since the account holder's machine

was last checked then the session validator sends a response to the client authenticator asking to check the account holder's hardware key attached to the computer. The hardware key is checked by the access device interface, which reads digital information associated with the hardware key. If the information is successfully read then the session is renewed and the time information is updated. If the information is not successfully read then an error message is sent to the login interface and a login enforcer makes the account holder login. (Col. 18, lines 6-45.) Therefore, Gregg creates a time-out operation to ensure that periodic re-authentication of a hardware key is performed. However, Gregg does not include a credential string and does not include a credential string validation component that checks whether the credential string has been previously received for validation within a predetermined time period.

The present invention is clearly different than Gregg, as articulated at page 9 of the specification. The present invention includes a portal that sends a session ID derivative as a credential string and UserID, produced as an encrypted hash of the active user's session ID, to a Target Application (TA) Proxy where the TA Proxy checks whether the UserID and credentials have been received recently (i.e., a predetermined time period). If not received recently then the UserID and credential string are sent to the TA. If, however, the UserID and credential string have been recently received and a second request with the same UserID and credential string is received by the TA Proxy then procedures associated with a network security breach may be initiated. The procedures may include terminating all the sessions authenticated by the compromised credential string. Therefore, the present invention checks whether the credential string has been previously received for validation within a predetermined time period to, in part, prevent security breaches occurring when a second request is received following a first request, which is clearly different then Gregg. Accordingly, Applicants submit claim 15 is not obvious over Azuma in view of Gregg.

Dependent Claims

Applicants submit that claims 3-8, 10, 13, 14, 16-19, and 21 depend from an allowable base claims. As such, claims 3-8, 10, 13, 14, 16-19, and 21 include the features of the base claims. Accordingly, Applicants respectfully submit that claims 3-8, 10, 13, 14, 16-19, and 21 include allowable subject matter and that the rejection over claims 3-8, 10, 13, 14, 16-19, and 21 be withdrawn.

Claims 5 and 14

Claim 5 recites, in pertinent part:

> ... wherein the sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory.

Claim 14 recites, in pertinent part:

> ... wherein the UserID is validated in the validating step and the password is maintained at the portal and used to process the confirmation request.

Applicants submit that claims 5 and 14 are not obvious for the reasons articulated above. In particular, Applicants agree with the Examiner's assertion on page 5 of the Office Action that Azuma does not maintain a password at a portal and does not keep the password from being sent to authenticate the UserID. However, Applicants submit Gregg does not make up for the deficiencies of Azuma because Gregg sends all of the login parameters, including a password, to a secure transaction server and then to a transaction clearinghouse. Therefore, Gregg does not maintain a password at a portal and does not keep the password from being sent to authenticate the UserID. Accordingly, claims 5 and 14 are not obvious in view of Azuma and Gregg.

Claims 6 and 19

Claim 6 recites, in pertinent part:

> ... checking whether the session ID and the credential string have been previously received within a predetermined time period...

Claim 19 recites, in pertinent part:

> ... further comprising a software application proxy which receives the UserID and the credential string and detects whether the UserID and the credential string have been previously received within a predetermined time period.

Applicants agree with the Examiner's assertions on pages 6 and 8 of the Office Action, which acknowledges that Azuma does not include a credential string previously received within a predetermined time period. However, Applicants submit Gregg does not make up for the deficiencies of Azuma. As explained when traversing the rejection over claim 15, Gregg creates a time-out operation to ensure that periodic re-authentication of a hardware key is performed, which is different from the present invention. Accordingly, Applicants submit claims 6 and 19 are not obvious in view of Azuma and Gregg.

***Other Matters***

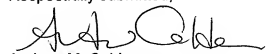
Claims 23-25 are added for the Examiner's consideration. The subject matter of claims 23-25 are allowable by virtue of their dependency on claim 15. Also, no combination of the applied references teach or suggest the features of claims 23-25.

**CONCLUSION**

In view of the foregoing amendments and remarks, Applicants submit that all of the claims are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue. The Examiner is invited to contact the undersigned at the telephone number listed below, if needed. Applicants hereby makes a written conditional petition for

extension of time, if required. Please charge any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 09-0457.

Respectfully submitted,



Andrew M. Calderon
Registration No. 38,093

Greenblum & Bernstein, P.L.C.
1950 Roland Clarke Place
Reston, Virginia 20191
Telephone: 703-716-1191
Facsimile: 703-716-1180